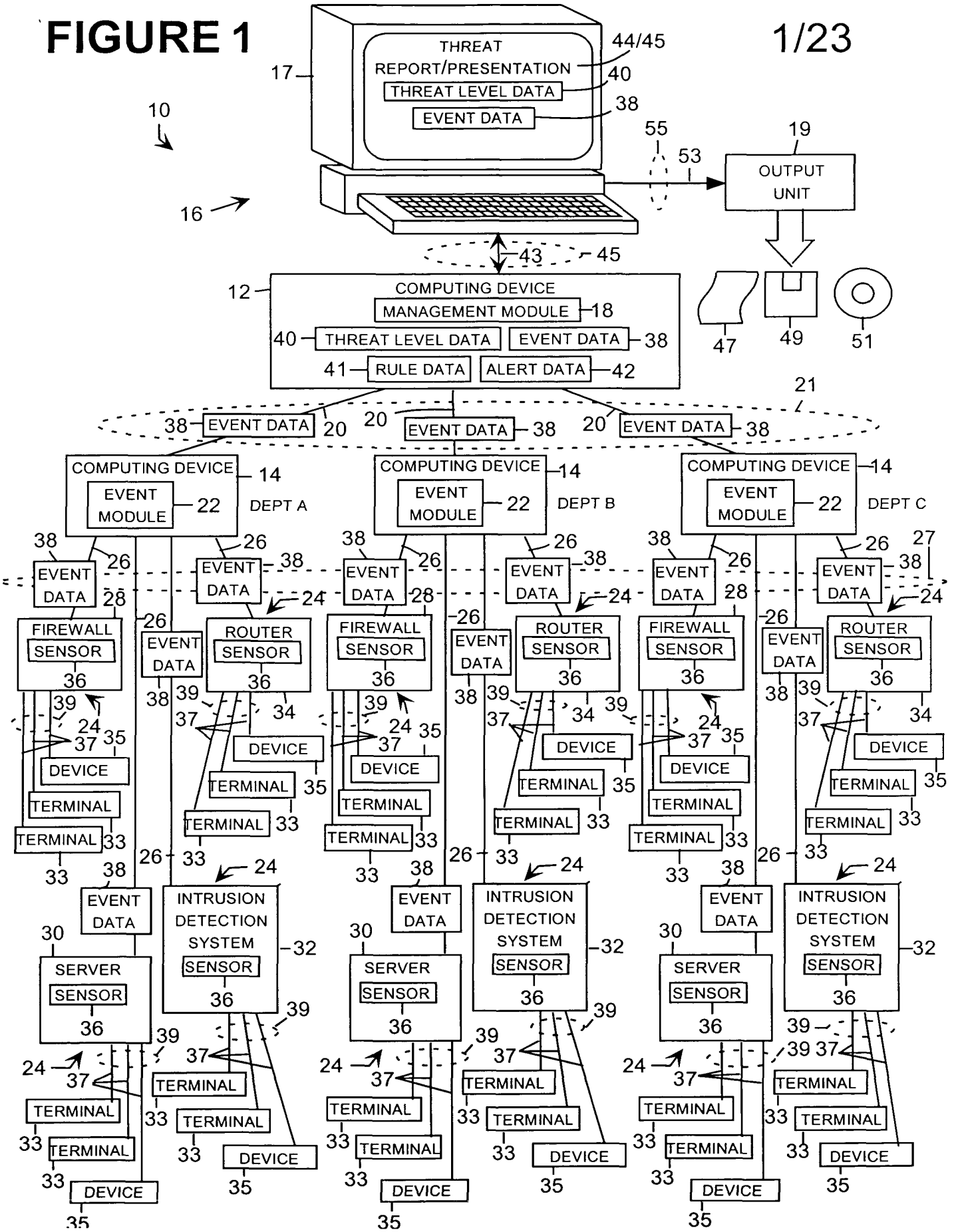
FIGURE 1


THREAT REPORT/PRESENTATION
44/45
THREAT LEVEL DATA
40
EVENT DATA
38
17
10
16
55
53
19
OUTPUT UNIT
43
45
12
COMPUTING DEVICE
MANAGEMENT MODULE
18
THREAT LEVEL DATA
EVENT DATA
RULE DATA
ALERT DATA
41
42
47
49
51
21
20
COMPUTING DEVICE
EVENT MODULE
22
14
DEPT A
DEPT B
DEPT C
EVENT DATA
26
28
24
FIREWALL SENSOR
ROUTER SENSOR
36
DEVICE
TERMINAL
33
35
37
39
34
INTRUSION DETECTION SYSTEM
SENSOR
32
SERVER
30

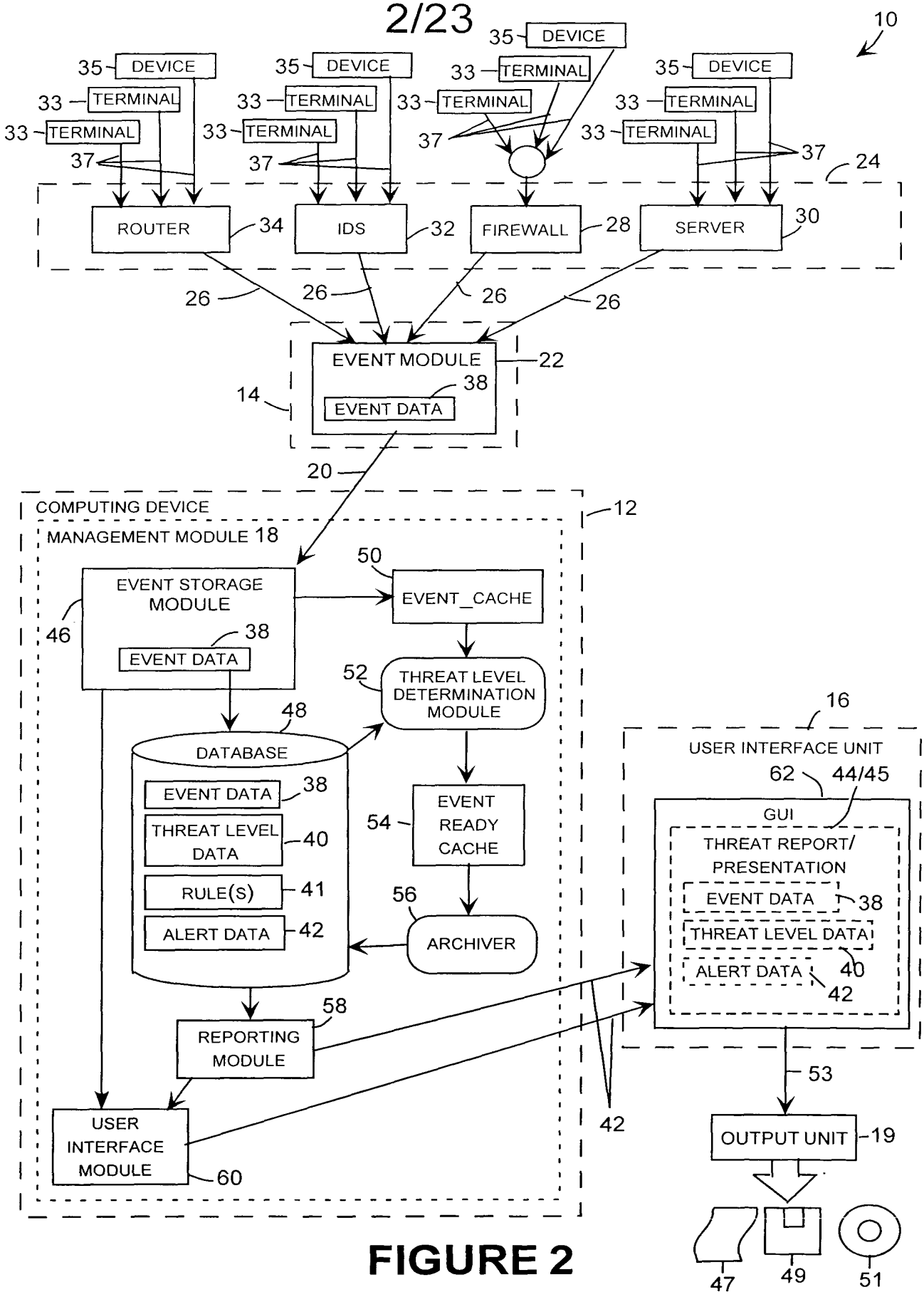

10
35 DEVICE
33 TERMINAL
37
24
ROUTER
34
IDS
32
FIREWALL
28
SERVER
30
26
EVENT MODULE
22
38
EVENT DATA
14
20
COMPUTING DEVICE
12
MANAGEMENT MODULE 18
EVENT STORAGE MODULE
46
50
EVENT_CACHE
52
THREAT LEVEL DETERMINATION MODULE
48
DATABASE
EVENT DATA
THREAT LEVEL DATA
40
RULE(S)
41
ALERT DATA
42
54
EVENT READY CACHE
56
ARCHIVER
58
REPORTING MODULE
USER INTERFACE MODULE
60
16
USER INTERFACE UNIT
62
44/45
GUI
THREAT REPORT/ PRESENTATION
53
OUTPUT UNIT
19
47
49
51

FIGURE 2

SINGLE MANAGEMENT MODULE AND MULTIPLE EVENT MODULES

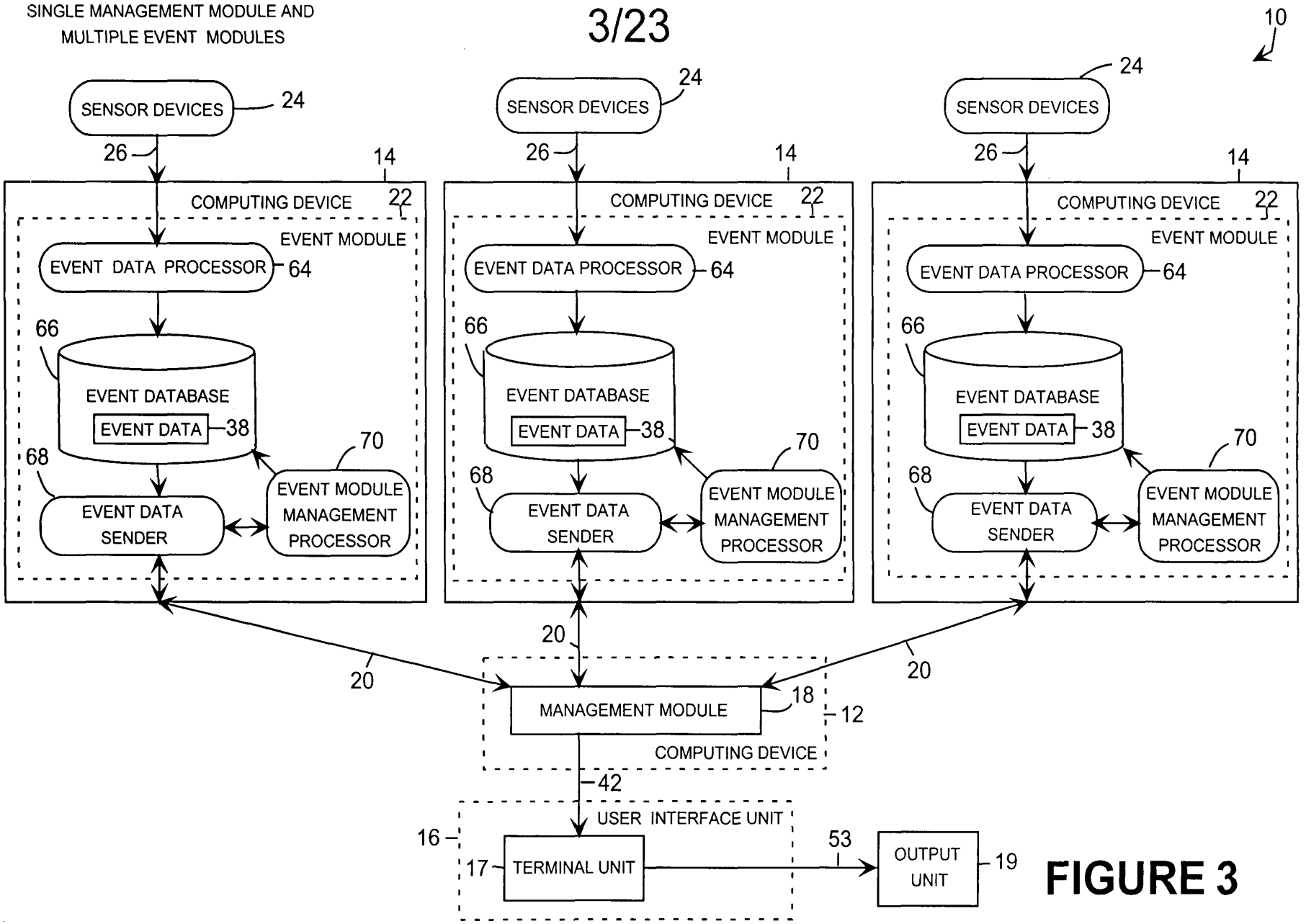


FIGURE 3

SINGLE MANAGEMENT MODULE AND
REDUNDANT EVENT MODULES

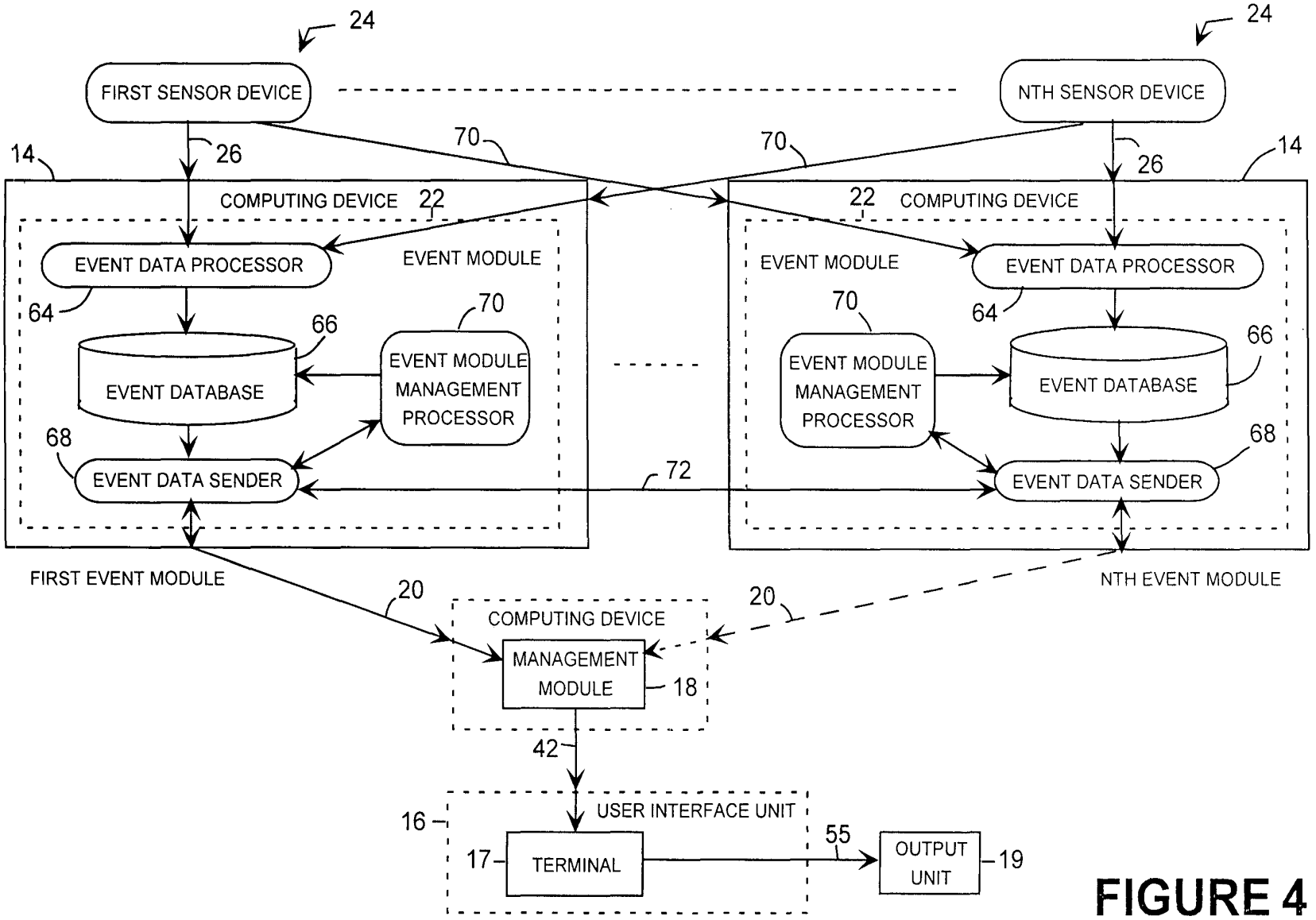


FIGURE 4

FIGURE 5

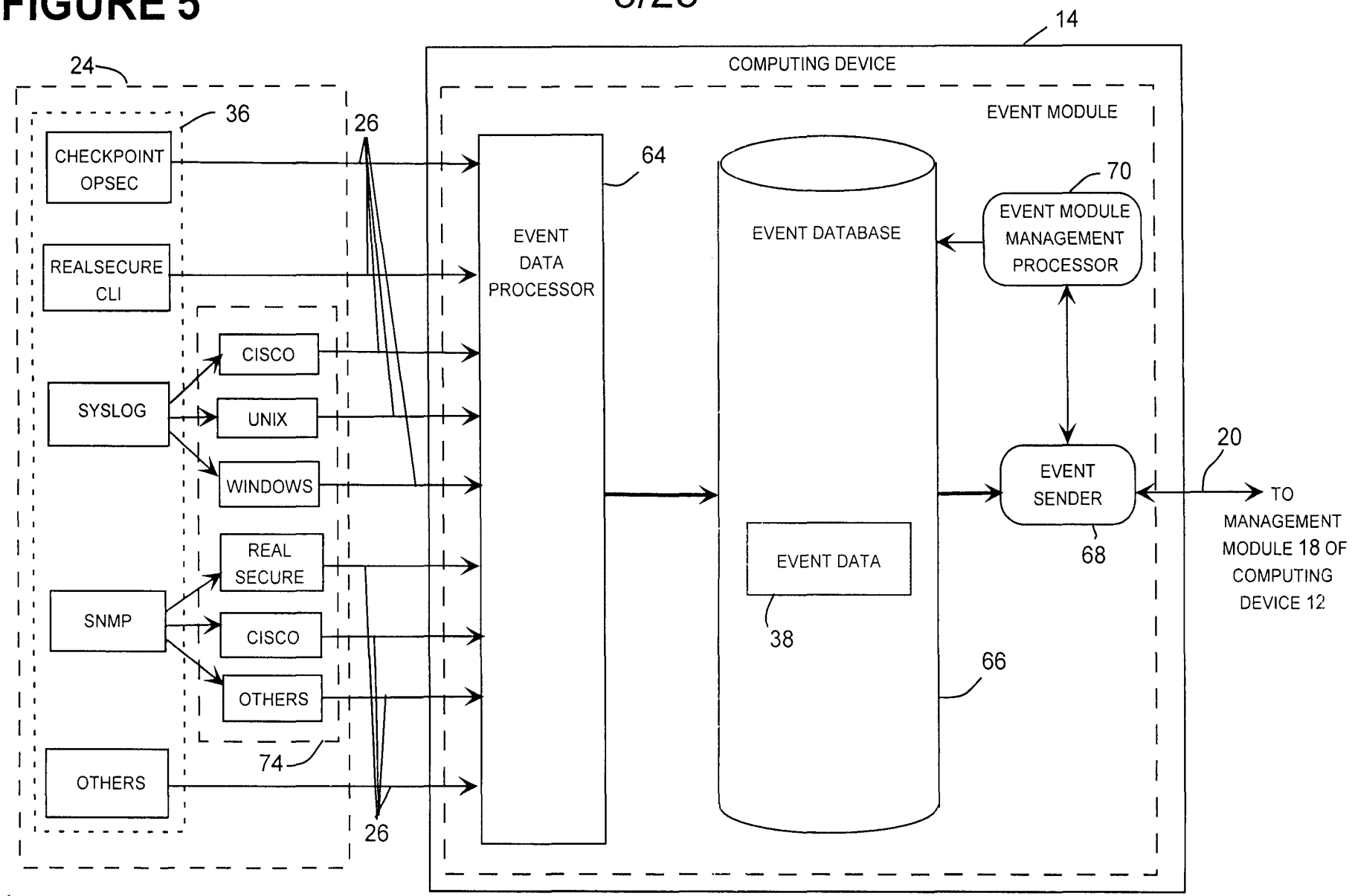

14
COMPUTING DEVICE
24
36
26
EVENT MODULE
CHECKPOINT OPSEC
REALSECURE CLI
SYSLOG
CISCO
UNIX
WINDOWS
REAL SECURE
SNMP
CISCO
OTHERS
OTHERS
74
26
64
EVENT DATA PROCESSOR
EVENT DATABASE
EVENT DATA
38
66
70
EVENT MODULE MANAGEMENT PROCESSOR
EVENT SENDER
68
20
TO MANAGEMENT MODULE 18 OF COMPUTING DEVICE 12

FIGURE 6

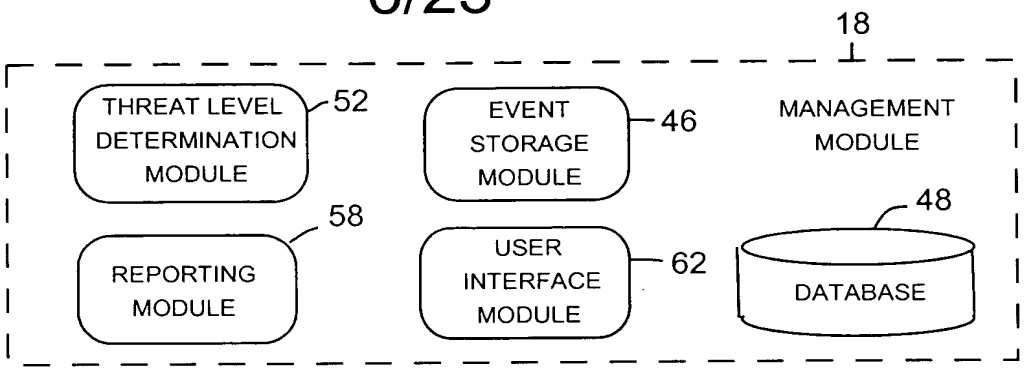


FIGURE 7

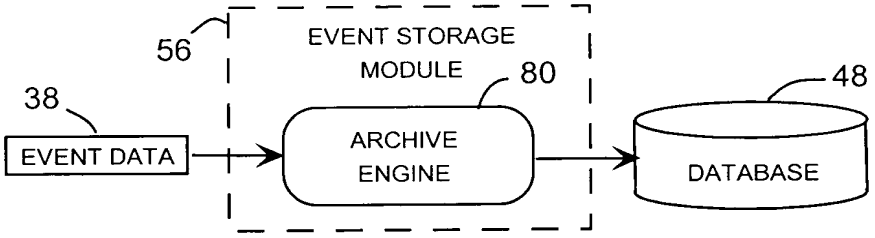


FIGURE 8

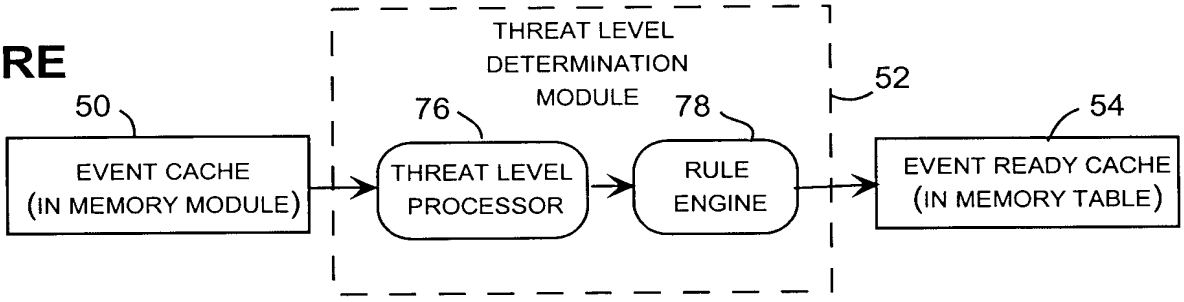


FIGURE 9

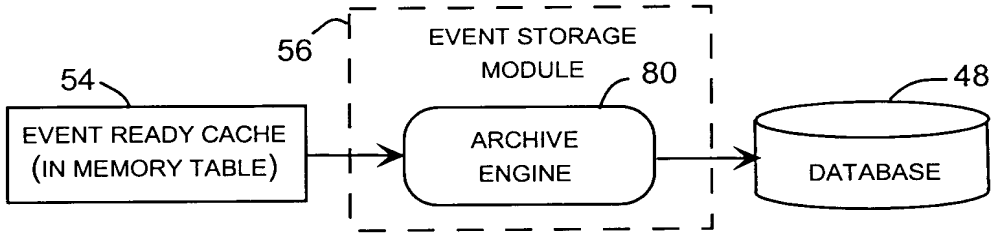


FIGURE 10

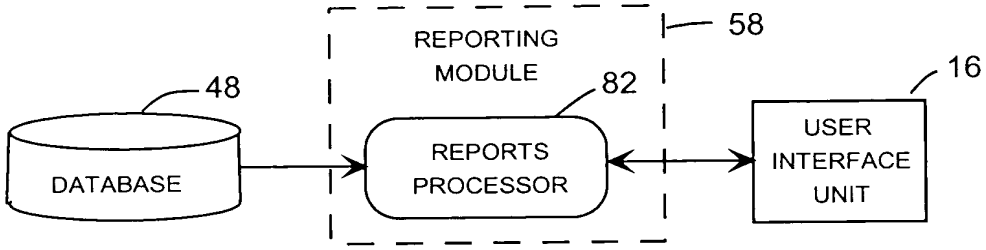


FIGURE 11

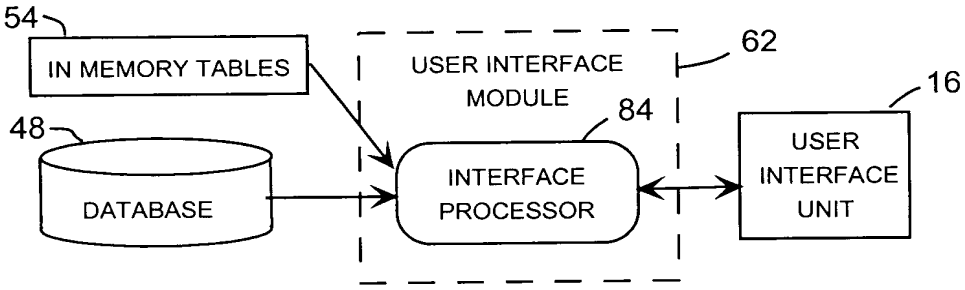


FIGURE 12

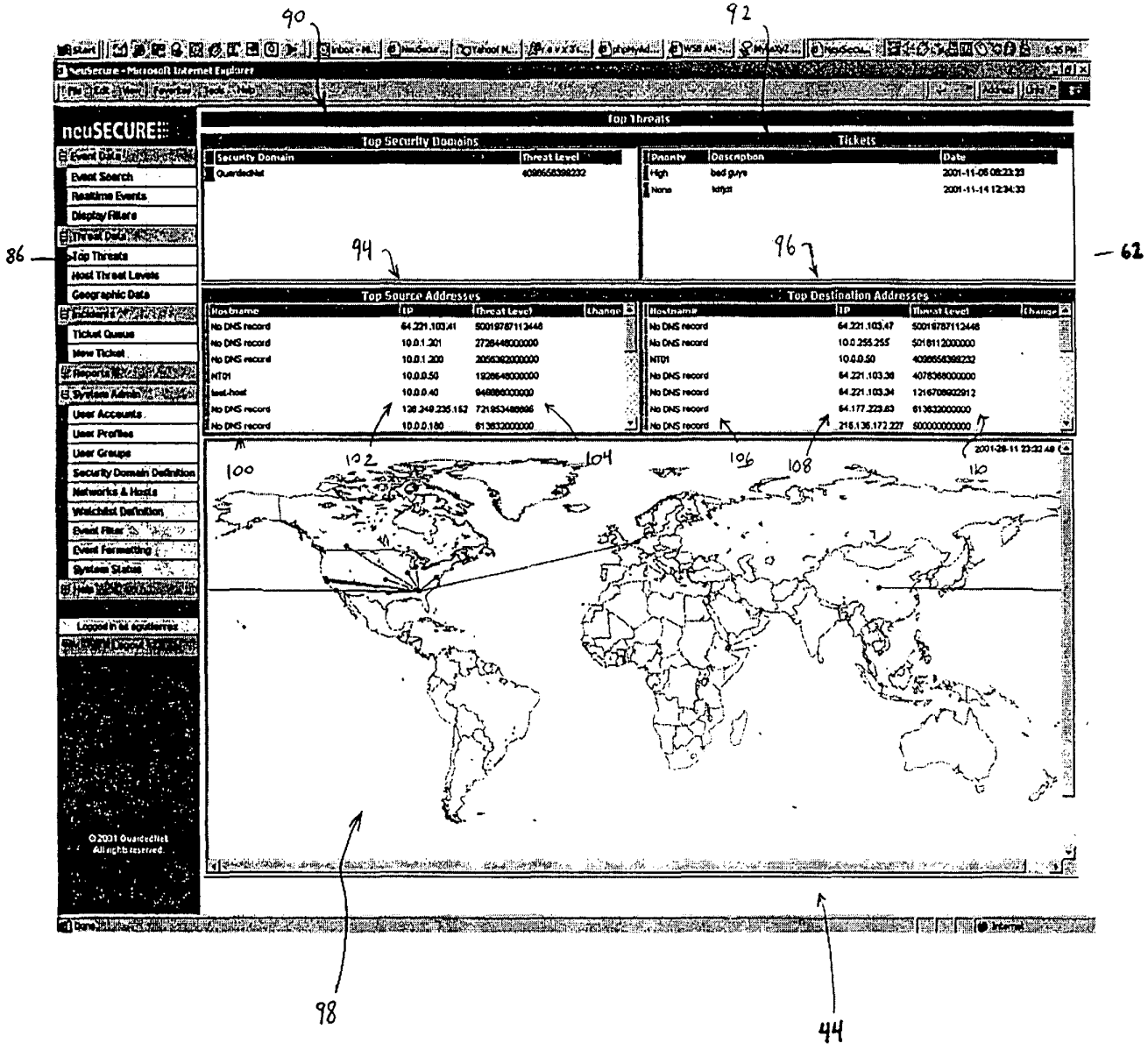

90
92
86
62
94
96
98
44
100
102
104
106
108
110
neuSECURE
Top Threats
Top Security Domains
Tickets
Top Source Addresses
Top Destination Addresses
Event Search
Realtime Events
Display Filters
Top Threats
Host Threat Levels
Geographic Data
Ticket Queue
New Ticket
User Accounts
User Profiles
User Groups
Security Domain Definition
Networks & Hosts
Watchlist Definition
Event Filter
Event Formatting
System Status

FIGURE 13

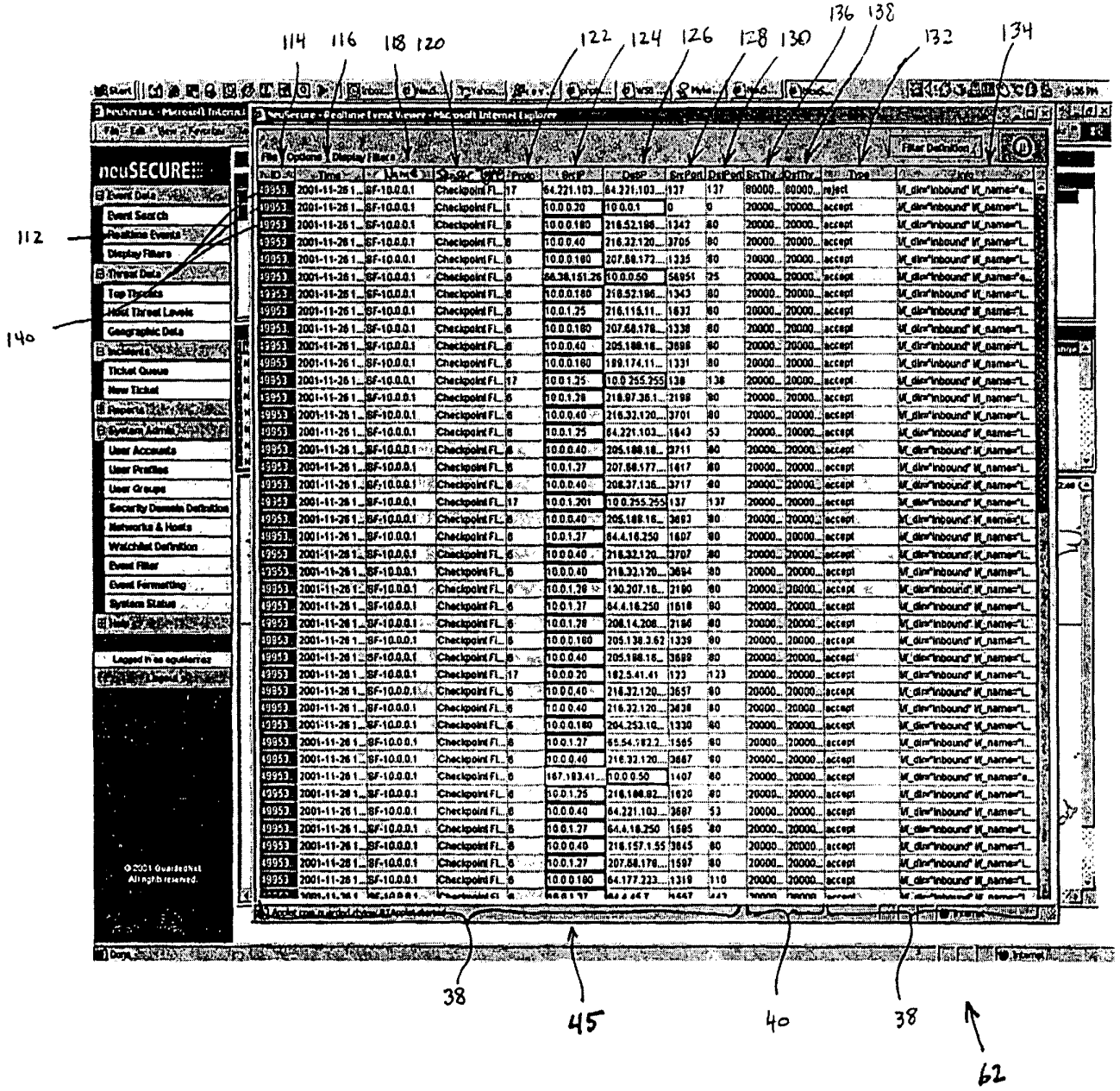

114
116
118
120
122
124
126
128
130
136
138
132
134
112
140
38
45
40
38
62

FIGURE 14

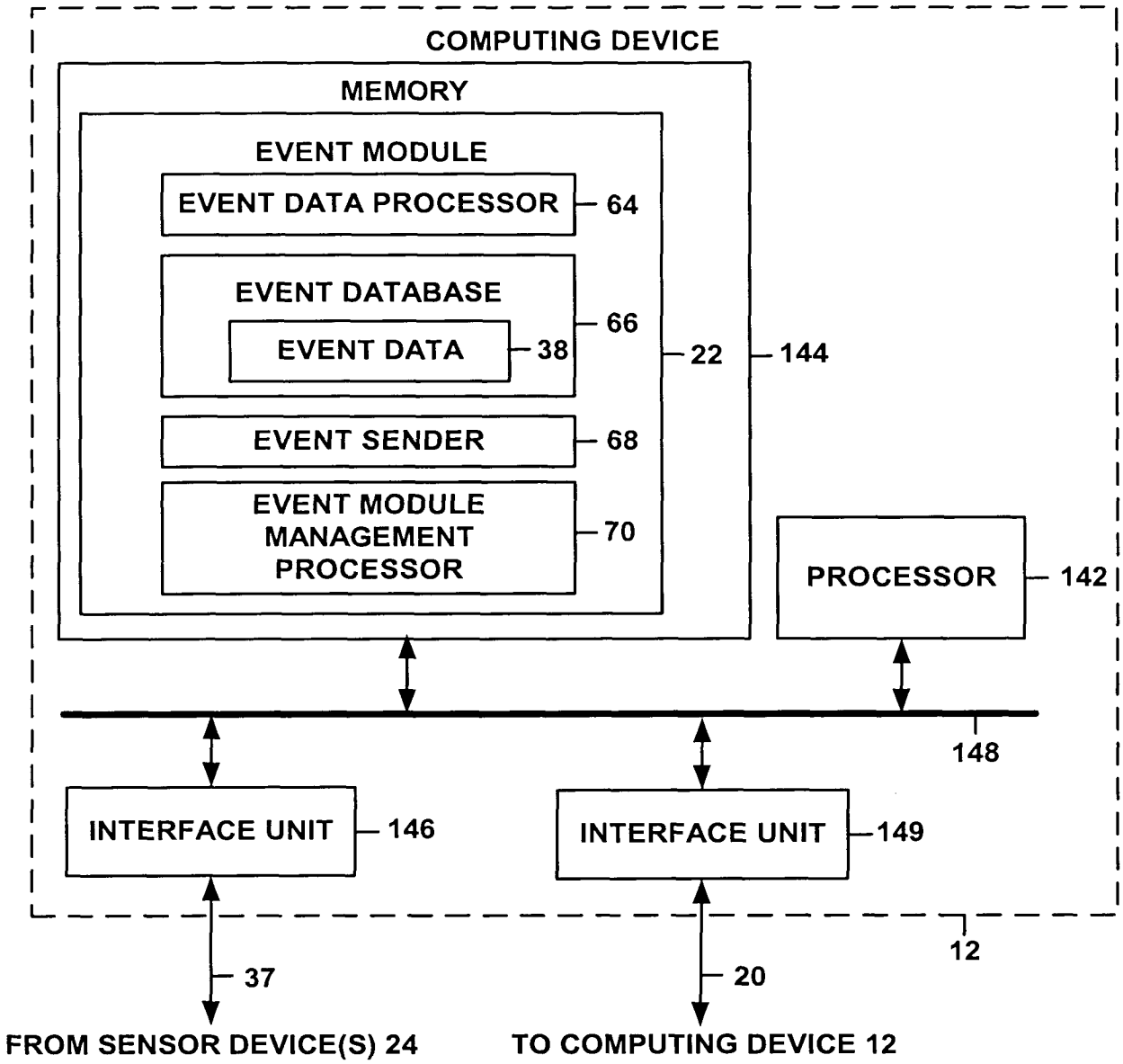

COMPUTING DEVICE
MEMORY
EVENT MODULE
EVENT DATA PROCESSOR
64
EVENT DATABASE
EVENT DATA
38
66
22
144
EVENT SENDER
68
EVENT MODULE MANAGEMENT PROCESSOR
70
PROCESSOR
142
148
INTERFACE UNIT
146
INTERFACE UNIT
149
12
37
20
FROM SENSOR DEVICE(S) 24
TO COMPUTING DEVICE 12

FIGURE 15

PROCESSING OF EVENT DATA BY EVENT MODULE

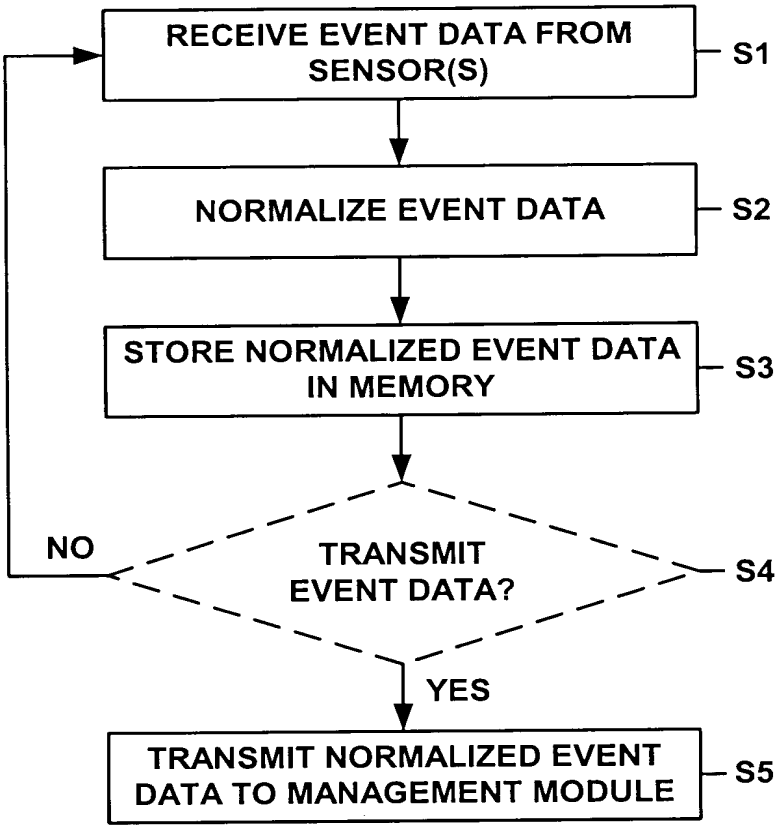


FIGURE 16

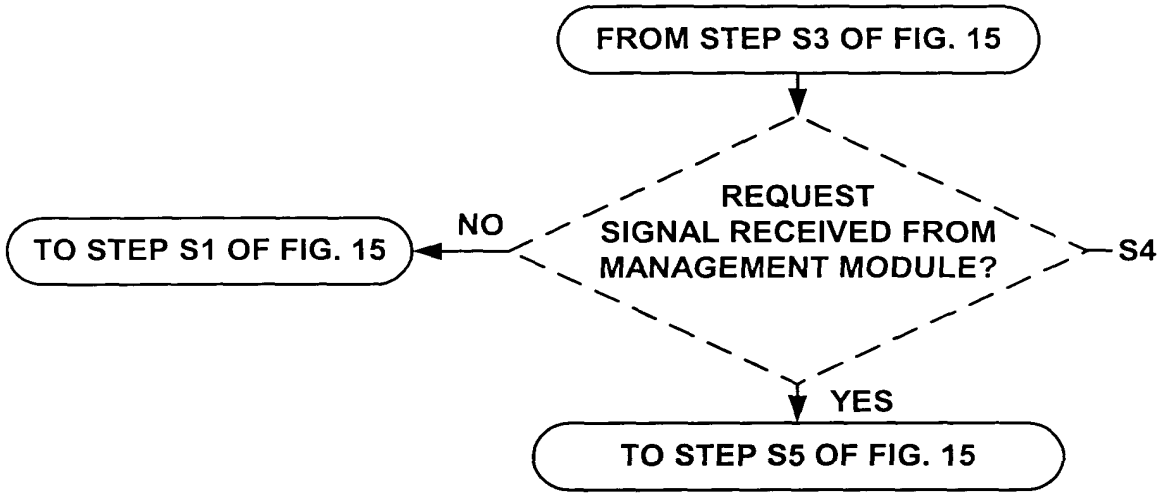


FIGURE 17

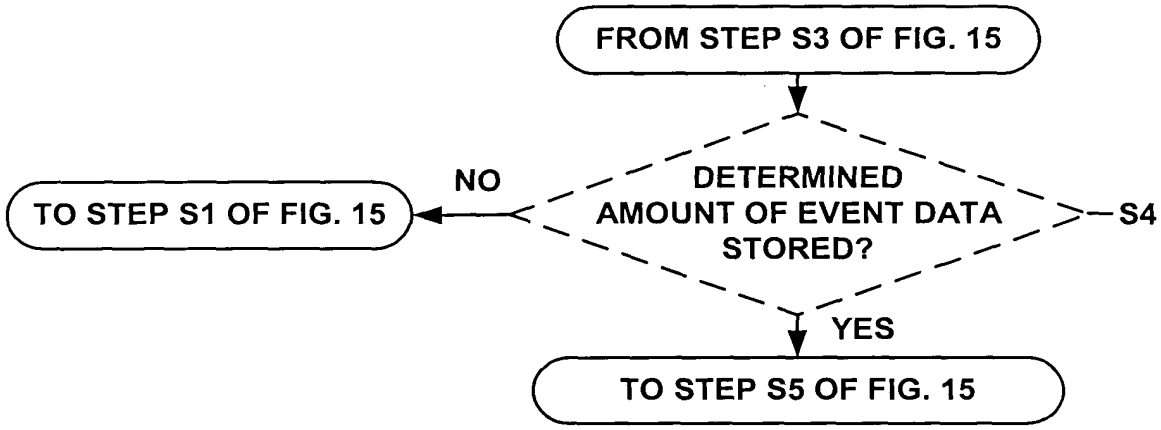


FIGURE 18

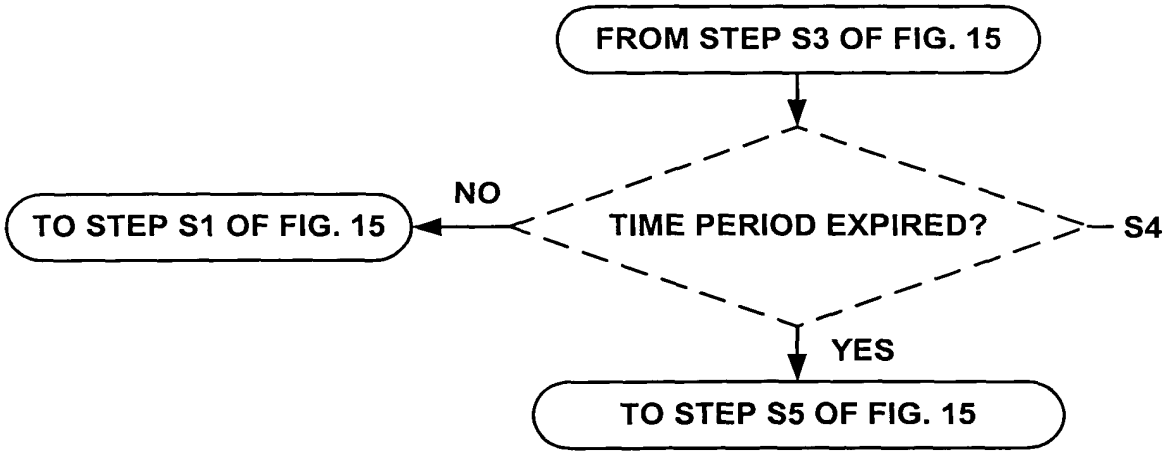


FIGURE 19

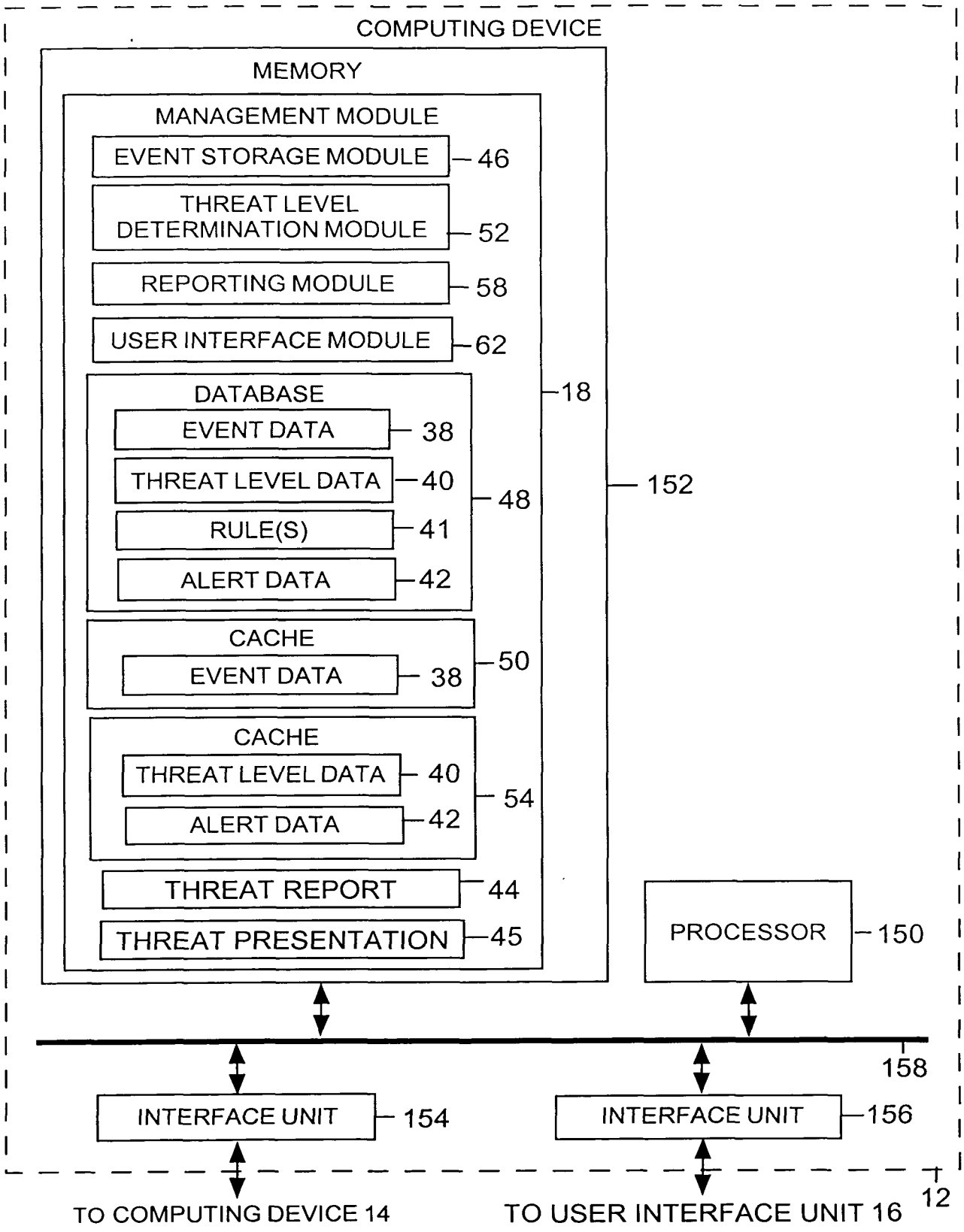

COMPUTING DEVICE
MEMORY
MANAGEMENT MODULE
EVENT STORAGE MODULE
46
THREAT LEVEL DETERMINATION MODULE
52
REPORTING MODULE
58
USER INTERFACE MODULE
62
DATABASE
EVENT DATA
38
THREAT LEVEL DATA
40
RULE(S)
41
ALERT DATA
42
48
18
CACHE
EVENT DATA
38
50
CACHE
THREAT LEVEL DATA
40
ALERT DATA
42
54
THREAT REPORT
44
THREAT PRESENTATION
45
152
PROCESSOR
150
158
INTERFACE UNIT
154
INTERFACE UNIT
156
12
TO COMPUTING DEVICE 14
TO USER INTERFACE UNIT 16

FIGURE 20

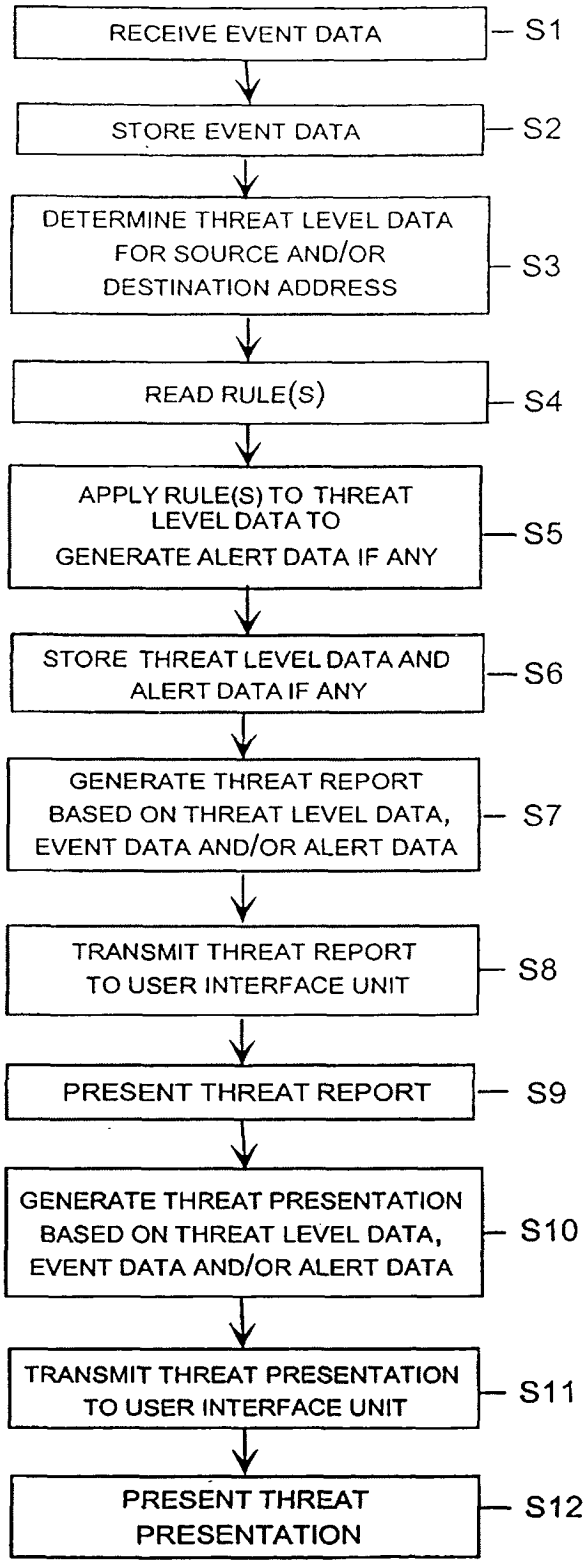

RECEIVE EVENT DATA
S1
STORE EVENT DATA
S2
DETERMINE THREAT LEVEL DATA FOR SOURCE AND/OR DESTINATION ADDRESS
S3
READ RULE(S)
S4
APPLY RULE(S) TO THREAT LEVEL DATA TO GENERATE ALERT DATA IF ANY
S5
STORE THREAT LEVEL DATA AND ALERT DATA IF ANY
S6
GENERATE THREAT REPORT BASED ON THREAT LEVEL DATA, EVENT DATA AND/OR ALERT DATA
S7
TRANSMIT THREAT REPORT TO USER INTERFACE UNIT
S8
PRESENT THREAT REPORT
S9
GENERATE THREAT PRESENTATION BASED ON THREAT LEVEL DATA, EVENT DATA AND/OR ALERT DATA
S10
TRANSMIT THREAT PRESENTATION TO USER INTERFACE UNIT
S11
PRESENT THREAT PRESENTATION
S12

FIGURE 21

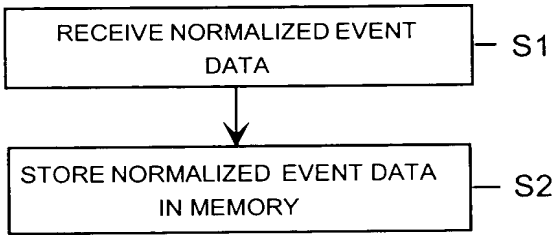


FIGURE 22

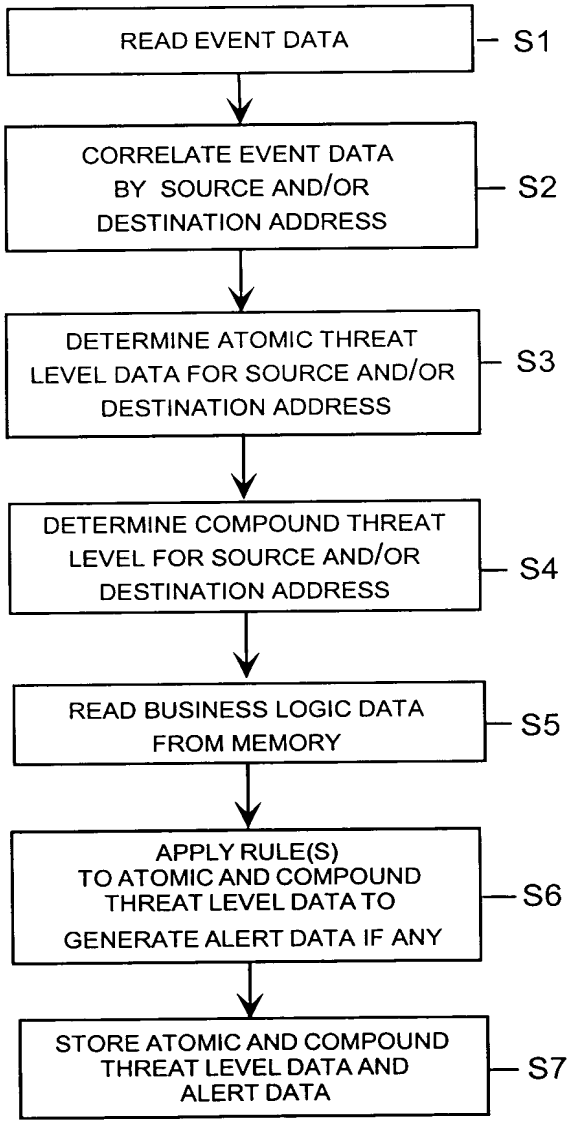


FIGURE 23

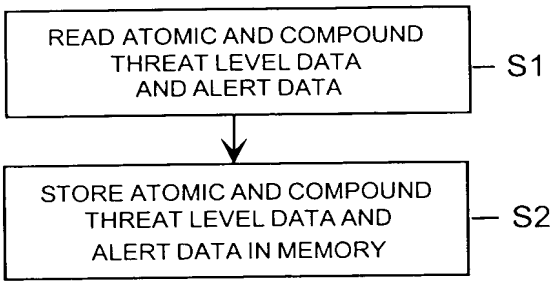


FIGURE 24

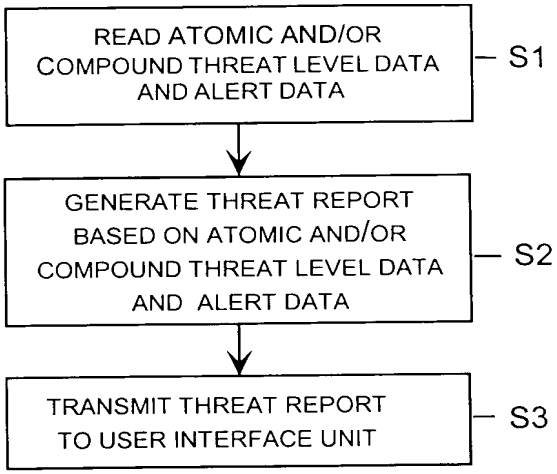


FIGURE 25

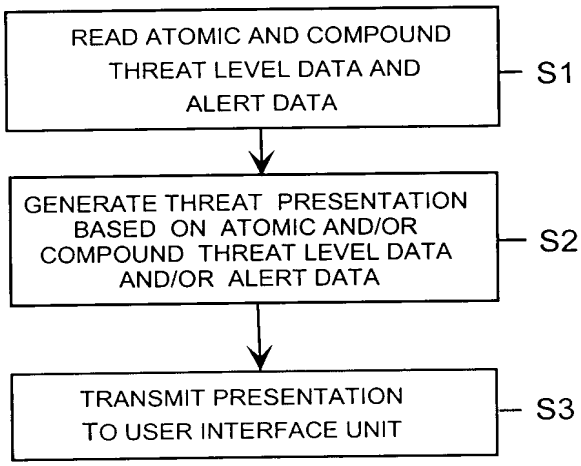


FIGURE 26

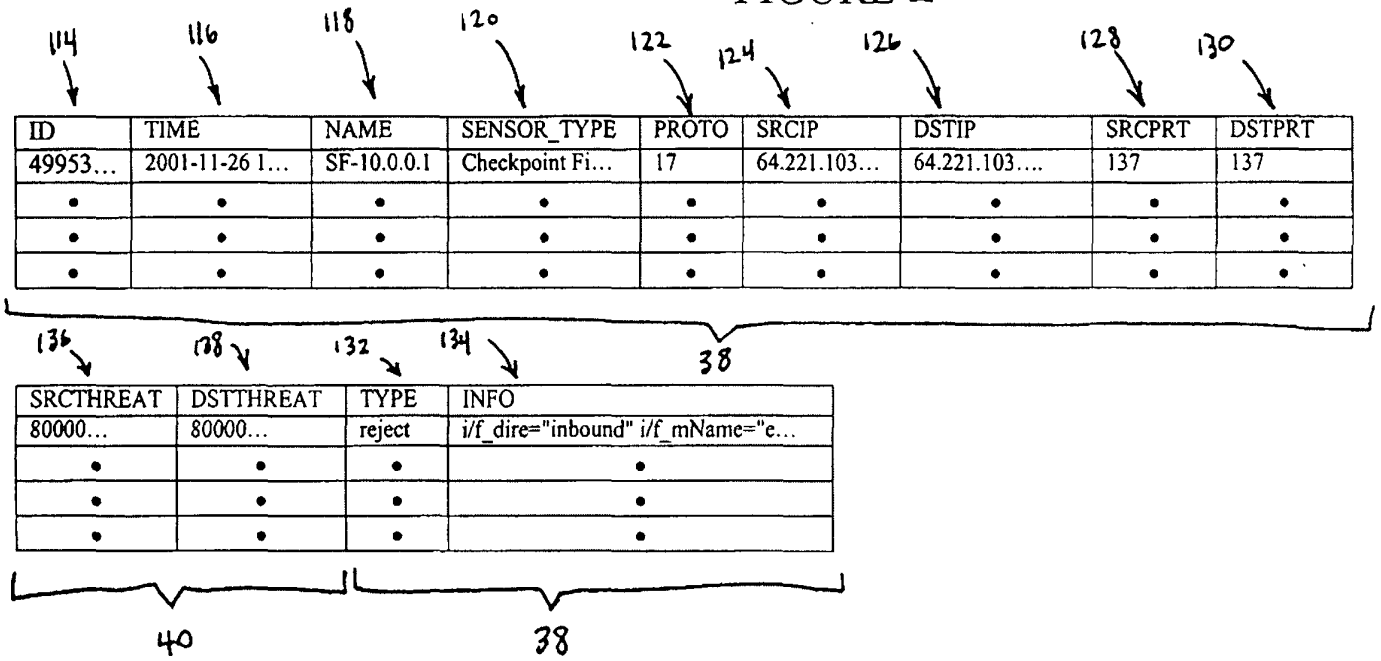

114
116
118
120
122
124
126
128
130
ID
TIME
NAME
SENSOR_TYPE
PROTO
SRCIP
DSTIP
SRCPRT
DSTPRT
49953...
2001-11-26 1...
SF-10.0.0.1
Checkpoint Fi...
17
64.221.103...
64.221.103....
137
137
38
136
138
132
134
SRCTHREAT
DSTTHREAT
TYPE
INFO
80000...
80000...
reject
i/f_dire="inbound" i/f_mName="e...
40
38

FIGURE 27

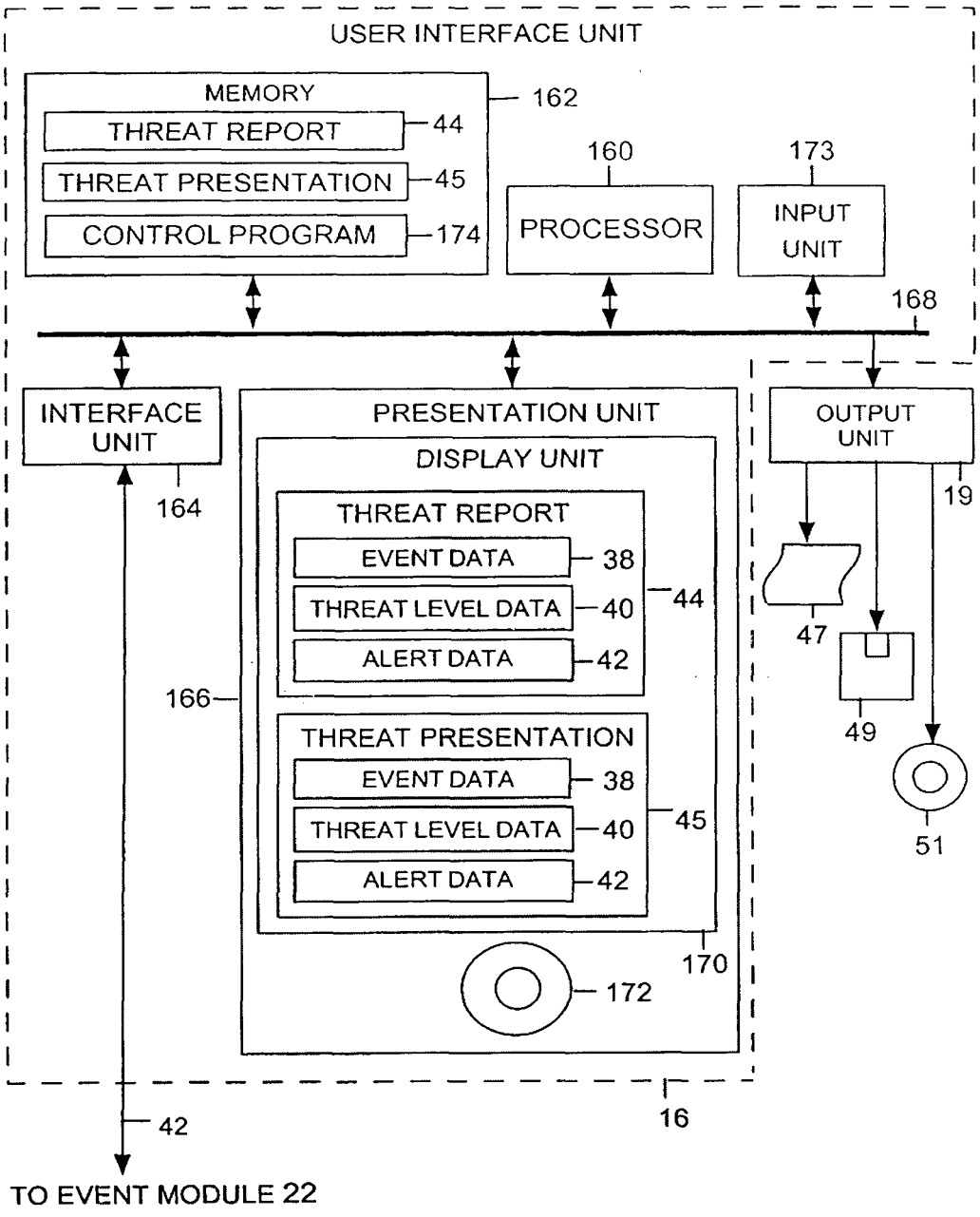

USER INTERFACE UNIT
MEMORY
162
THREAT REPORT
44
THREAT PRESENTATION
45
CONTROL PROGRAM
174
160
PROCESSOR
173
INPUT UNIT
168
INTERFACE UNIT
164
PRESENTATION UNIT
DISPLAY UNIT
THREAT REPORT
EVENT DATA
38
THREAT LEVEL DATA
40
ALERT DATA
42
44
166
THREAT PRESENTATION
EVENT DATA
38
THREAT LEVEL DATA
40
ALERT DATA
42
45
170
172
OUTPUT UNIT
19
47
49
51
16
42
TO EVENT MODULE 22

FIGURE 28

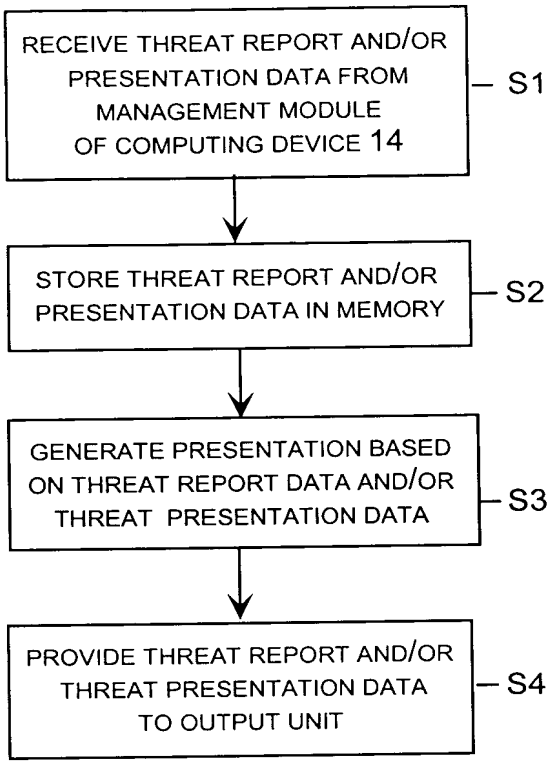

RECEIVE THREAT REPORT AND/OR PRESENTATION DATA FROM MANAGEMENT MODULE OF COMPUTING DEVICE 14
S1
STORE THREAT REPORT AND/OR PRESENTATION DATA IN MEMORY
S2
GENERATE PRESENTATION BASED ON THREAT REPORT DATA AND/OR THREAT PRESENTATION DATA
S3
PROVIDE THREAT REPORT AND/OR THREAT PRESENTATION DATA TO OUTPUT UNIT
S4

FIGURE 29

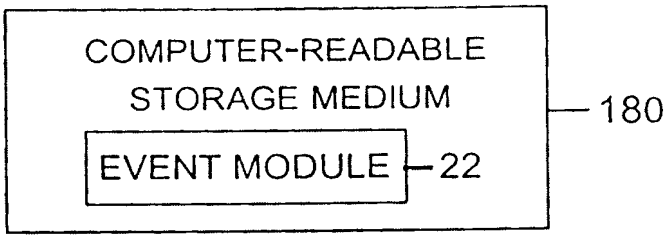


FIGURE 30

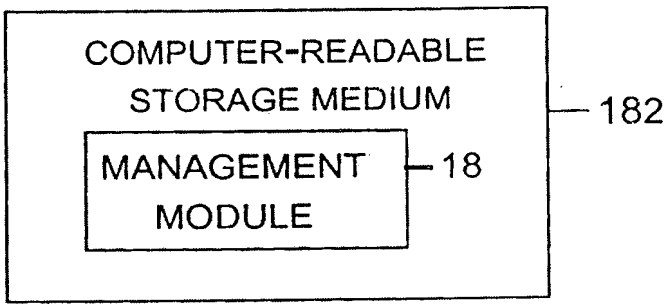
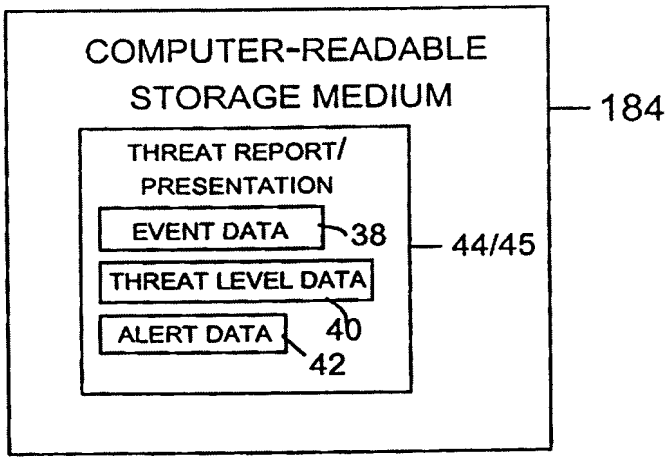


FIGURE 31



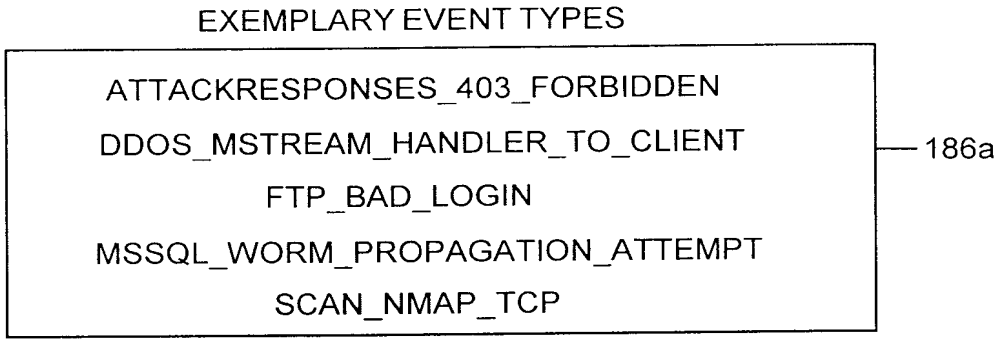


FIGURE 32A

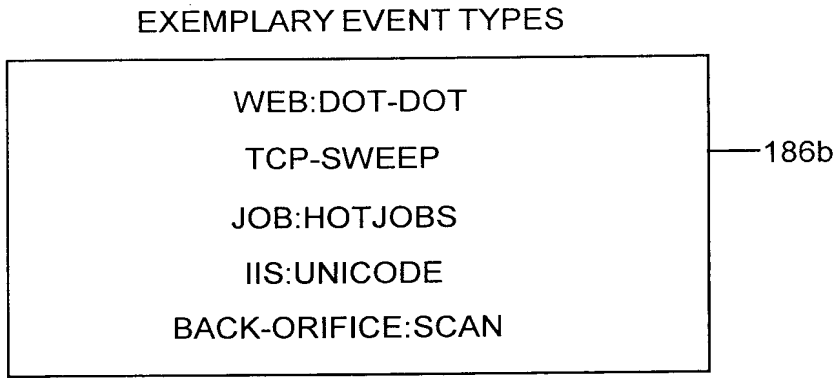


FIGURE 32B

CALCULATIONS

190 THREAT

$T(H) = TW[H] * NB\text{-}TW[NB[H]]$

192 SOURCE THREAT

$ST(e) = T(e.src)$

194 DESTINATION THREAT

$DT(e) = T(e.dst)$

196 VULNERABILITY

$DT(e) = T(e.dst)$

198 EVENT VALIDITY

$EV(e) = VALIDITY[e.src][e.type]$

200 EVENT SEVERITY

$ES(e) = PRIORITY[e]$

202 ATOMIC THREAT LEVEL

$AT(e) = EV(e) * V(e) * ST(e) * ES(e)$

204 HOST THREAT LEVEL

$$\delta(e,H,t) = \begin{cases} 1 \text{ if } (e.src = H \text{ or } e.dst = H) \\ 0 \text{ otherwise} \end{cases}$$

$$HT(H,t) = \frac{\sum_{i=1}^{N} AT(e_i) * \delta(e_i,H,t)}{\sum_{i=1}^{N} \delta(e_i,H,t)}$$

206 DIFFERENTIAL THREAT LEVEL

$$DTL(H,T_1,T_1) = \frac{HT(H_1,T_1)}{HT(H_1,T_2)} * \frac{T_2}{T_1} \quad \text{WHERE } 0<T_1<T_2$$

FIGURE 33

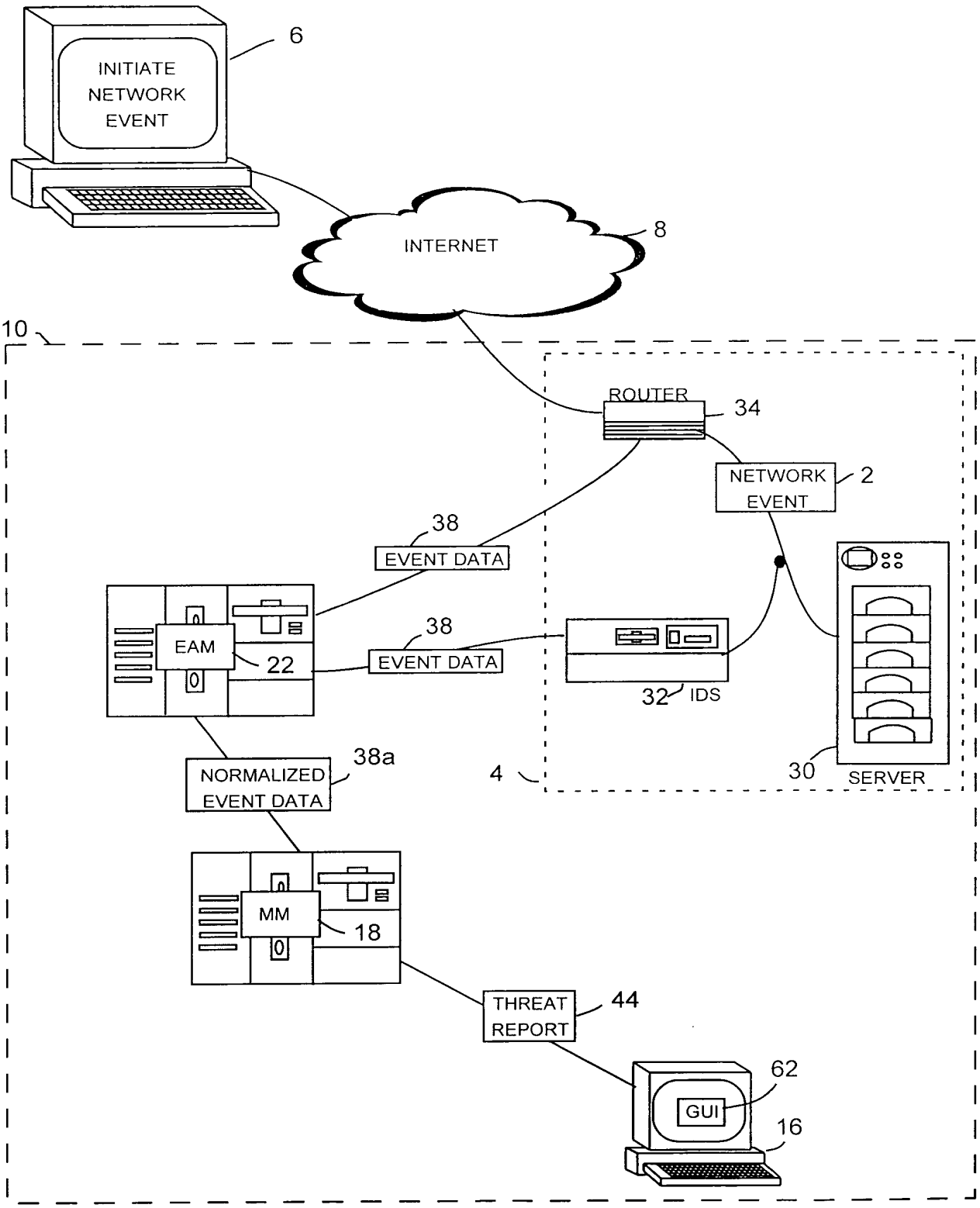

INITIATE NETWORK EVENT
6
INTERNET
8
10
ROUTER
34
NETWORK EVENT
2
38
EVENT DATA
EAM
22
38
EVENT DATA
32
IDS
30
SERVER
4
NORMALIZED EVENT DATA
38a
MM
18
THREAT REPORT
44
62
GUI
16

FIGURE 34